AMENDMENTS TO THE CLAIMS

- At time of the Action: Claims 1-8, 10, 12-16, 18, 19, 21-27, 30-38, 40, 42, 45, 46, 48, 49, and 51-55
- Amended Claims: Claims 1, 12, 13, 16, 23-25, 27, 31, 42, 46, 53, and 55
- Previously Canceled Claims: Claims 9, 11, 17, 20, 28, 29, 39, 41, 43, 44, 47, and 50
- Canceled Claims: Claims 3, 4, 14, 33, and 34
- New Claims: Claims 56-59
- After this Response: Claims 1, 2, 5-8, 10, 12, 13, 15, 16, 18, 19, 21-27, 30-32, 35-38, 40, 42, 45, 46, 48, 49, and 51-59

The following listing of claims replaces all prior versions and listings of claims in the application.

1. (Currently Amended) A method implemented on a supplemental television content server by a processor configured to execute instructions that, when executed by the processor, directs the supplemental television content server to perform acts ~~of signing a supplemental television content application comprising files, the method~~ comprising:

identifying at least a first portion of ~~the~~ files in an application as belonging to at least one cluster, wherein the application is a supplemental television content application comprising files carrying code and associated objects; wherein the cluster is a grouping of files;

determining a cluster signature for each cluster; [[and]]

developing an expression that includes the location of the cluster signature, and

storing the expression in a start file, wherein the start file carries application run parameters and references an application boot file to start execution of the application;

wherein a second portion of the files comprises a web page and determining a signature for each web page by determining at least one of:

developing a link to the signature and storing the link in the web page, or

storing the signature in the web page.

2. (Original) The method of claim 1 wherein said signature for each cluster is based on a hash code of the files composing the cluster.

3. (Canceled)

4. (Canceled)

5. (Original) The method of claim 1 further comprising storing at least one of delegate information, security policy information, time version information, and file identification information for each cluster in the expression.

6. (Original) The method of claim 1 further comprising storing the cluster signature in a signature file, developing a reference to the files composing the cluster, and storing the reference to the files in the signature file.

7. (Original) The method of claim 1 further comprising storing the cluster signature in a signature file, developing a time version record for the cluster, and storing the time version record in the signature file.

8. (Original) The method of claim 1 further comprising developing at least one of a reference to the files composing the cluster, and a time version record for the cluster.

9. (Previously Canceled)

10. (Previously Presented) The method of claim 1 wherein the web pages is at least one of a markup language based application and dynamically created by a client.

11. (Previously Canceled)

12. (Currently Amended) A method ~~of signing a supplemental television content application comprising files, the method~~ implemented on a supplemental television content

server by a processor configured to execute instructions that, when executed by the processor, directs the supplemental television content server to perform acts comprising:

identifying a first portion of ~~the~~ files that together compose a dynamic web page, wherein the dynamic web page is a supplemental television content delivered through an interconnecting channel separate from a channel used to deliver broadcast media and a content of the dynamic web page changes during a time interval;

determining a signature for the dynamic web page;

storing one of a link to the signature in the dynamic web page, or the signature in the dynamic web page; and

developing an expression that includes signature information, and storing the expression in the dynamic web page as extensible markup language (XML) metadata,

wherein the expression comprises at least one of security policy information data or delegate data,

wherein the security policy information data comprises at least one of specifying a location of a permission request file that indicates allowed and disallowed operations for the application and defining a location of a privacy statement,

wherein the delegate data includes identities and constraints of a delegate, and

wherein a delegate is an entity that is authorized to sign portions of the application in addition to a main signer.

13. (Currently Amended) The method of claim 12 wherein,

~~the metadata is extensible markup language (XML) metadata,~~

a syntactical extension of an XML link element provides reverse linkage between an XML document and the signature by using a link rev= tag, and

the signature is composed of a Reference element, a KeyInfo element, a DigestValue element, a SignatureValue element, and a VersionNumber element, wherein the VersionNumber element provides versions for signature files under a separate namespace, using a SignatureProperties element.

14. (Canceled)

15. (Original) The method of claim 12 further comprising:

clustering at least a second portion of the files in at least one cluster;

determining a cluster signature for each cluster; and

developing an expression that includes indicating the location of the clusters.

16. (Currently Amended) A method ~~of executing a supplemental television content application that comprises files, the method~~ implemented on a supplemental television content server by a processor configured to execute instructions that, when executed by the processor, directs the supplemental television content server to perform acts comprising:

executing a supplemental television content application comprising files, wherein the files carry code and assorted objects;

determining if the files are arranged in a cluster, wherein a cluster is a subset of the files grouped through logical organization, and determining if any of the files are arranged in clusters comprises referencing a security information resource file contained within a start file, wherein the security information resource file comprises a cluster information metadata expression indicating the files that compose the cluster, wherein a signature location metadata expression indicating a location of a signature for the cluster; [[:]]

determining if ~~an~~ the application start file has a record that includes one of a reference to an expression having a location of the signature, and the expression, wherein the start file carries application run parameters and references an application boot file to start execution of the supplemental television content application ~~is a file that describes parameters to execute an associated application~~;

reading from the expression the location of a file having a signature of a cluster for each cluster, wherein the reading operation further comprises reading whether there are any delegates for any of the clusters, and determining if a signature is valid based on the delegates wherein a delegate is an entity that is authorized to sign portions of the application in addition to a main signer;

determining if the signatures can be verified;

determining the identify of all clusters that comprise the application;

~~for each cluster, determining the location of the signature of the cluster by a signature location metadata expression;~~

~~determining the files that compose the cluster by a cluster information metadata expression;~~

determining a delegate name and constraints imposed on the authority of the delegate, wherein the constraints comprise time boundaries; and

verifying the integrity of the files in the cluster by operations including verifying the signature.

17. (Previously Canceled)

18. (Previously Presented) The method of claim 16 wherein each of the files composing a cluster is stored in one of the expression, and a file storing a signature.

19. (Previously Presented) The method of claim 16 wherein each signature is based on a hash of each file composing the cluster.

20. (Previously Canceled)

21. (Previously Presented) The method of claim 16 further comprising reading time version information associated with a cluster and determining if the signature may be valid based on the time version information.

22. (Previously Presented) The method of claim 16 further comprising determining if the files is a web page file having one of a link to a signature and a signature; reading the signature, and verifying the signature.

23. (Currently Amended) A method ~~of executing a supplemental television content application comprising files, the method~~ implemented on a supplemental television content server by a processor configured to execute instructions that, when executed by the processor, directs the supplemental television content server to perform acts comprising:

executing a supplemental television content application comprising files, wherein the files carry code and assorted objects;

determining if the files compose web pages; and

if the files compose web pages, then

for each of the web pages, decoding the web page to determine if the web page has extensible markup language (XML) metadata comprising an <AppSecurityInfo> element indicating one of a link to a digital signature and a digital signature,

reading the signature, and

verifying the signature,

if any of the web pages lack the link to a digital signature, lack the digital signature, or the signatures is not verified then warn a user that a file has not been signed, warn the user that the signature is not valid, reject the file, or restrict access by the web page to system resources.

24. (Currently Amended) The method of claim 23 further comprising:

determining if the files are arranged in a cluster;

for each cluster, determining the files that compose the cluster and the location of the signature of the cluster; and

verifying the integrity of the files in the cluster by operations including verifying the signature.

25. (Currently Amended) A supplemental television content architecture comprising:

an application comprising a collection of files, wherein the application is a supplemental television application delivered through an interconnecting channel separate from a channel used to deliver broadcast media;

a cluster of the files, wherein the cluster is a subset of the files grouped through a logical organization,

the files comprising:

a signature file comprising a cluster signature, a reference to the files in the cluster, and a time version information;

a security information resource file comprising a cluster information metadata, a signature location metadata, and a delegate metadata; and

a start file including a link to the security information resource file or the security information file, wherein the start file carries application run parameters and references an application boot file to start execution of the application,

wherein the signature location metadata describes a location of the signature file by a link,

wherein the cluster signature includes a hash code of each of the files comprising the cluster and a digital signature for signing the hash code of each of the files,

wherein the time version information describes the version of the signature file as a function of the files in the cluster, and

wherein the delegate metadata comprises identity and constraints of a delegate.

26. (Previously Presented) The architecture of claim 25 wherein the security information resource file further comprises a policy declaration that specifies the location of a permission request file which indicates allowed and disallowed operations for the application and a policy declaration that defines the location of a privacy statement.

27. (Currently Amended) The architecture of claim 25 wherein the metadata is extensible markup language (XML) metadata,

a syntactical extension of an XML link element provides a reverse linkage between an XML document and the signature by using a link rev= tag, and

the signature is composed of a Reference element, a KeyInfo element, a DigestValue element, a SignatureValue element, and a VersionNumber element, wherein the VersionNumber element provides versions for signature files under a separate namespace, using a SignatureProperties element.

28. (Previously Canceled)

29. (Previously Canceled)

30. (Previously Presented) The architecture of claim 25 wherein the metadata expression comprises at least one of security policy information and signature delegate information.

31. (Currently Amended) One or more computer readable media having stored thereon a plurality of instructions that, when executed by at least one processor, causes the processor to perform acts comprising:

identifying at least a first portion of supplemental television content application files in at least one cluster, wherein a supplemental television content application comprises a start file carrying application run parameters and referencing an application boot file to start execution of the supplemental television content application;

determining a cluster signature for each cluster; [[and]]

developing an expression that includes the location of the signature, wherein a second portion of the files comprises a web page and further comprising determining a signature for each web page by determining at least one of:

developing a link to the signature and storing the link in the web page; or

storing the signature in the web page; and

storing at least one of expressions or a link to the expressions in the start file.

32. (Original) The computer readable media of claim 31 wherein the signature for each cluster is based on a hash code of the files composing the cluster.

33. (Canceled)

34. (Canceled)

35. (Original) The computer readable media of claim 31 wherein the expression further includes at least one of delegate information, security policy information, time version information, and file identification information for each cluster.

36. (Original) The computer readable media of claim 31 wherein said acts further comprises storing the cluster signature in a signature file, developing a reference to the files composing the cluster, and storing the reference to the files in the signature file.

37. (Original) The computer readable media of claim 31 wherein said acts further comprise storing the cluster signature in a signature file, developing a time version record for the cluster, and storing the time version record in the signature file.

38. (Original) The computer readable media of claim 31 wherein said acts further comprise developing at least one of a reference to the files composing the cluster, and a time version record for the cluster.

39. (Previously Canceled)

40. (Previously Presented) The computer readable media of claim 31 wherein the web pages is at least one of a markup language based application and dynamically created by a client.

41. (Previously Canceled)

42. (Currently Amended) One or more computer readable media having stored thereon a plurality of instructions that, when executed by at least one processor, causes the processor to perform acts comprising:

identifying a first portion of supplemental television content application files that together compose a dynamic web page, wherein the dynamic web page is a supplemental television content delivered through an interconnecting channel separate from a channel used to deliver broadcast media and a content of the dynamic web page changes during a time interval;

determining a signature for the dynamic web page;

storing one of a link to the signature in the dynamic web page, or the signature in the dynamic web page; and

developing an expression that includes signature information, and storing the expression in the dynamic web page as extensible markup language (XML) metadata,

wherein the expression comprises at least one of security policy information data or delegate data,

wherein the security policy information data comprises at least one of specifying a location of a permission request file that indicates allowed and disallowed operations for the application and defining a location of a privacy statement,

wherein the delegate data includes identities and constraints of a delegate, and

wherein a delegate is an entity that is authorized to sign portions of the application in addition to a main signer.

43. (Previously Canceled)

44. (Previously Canceled)

45. (Original) The computer readable media of claim 42 wherein said acts further comprise:

clustering at least a second portion of the files in at least one cluster;

determining a cluster signature for each cluster; and

developing an expression that includes indicating the location of the clusters.

46. (Currently Amended) One or more computer readable media having stored thereon a plurality of instructions that, when executed by at least one processor, causes the processor to perform acts comprising:

executing a supplemental television content application comprising files, wherein the files carry code and assorted objects;

determining if ~~supplemental television content application~~ the files are arranged in a cluster, wherein a cluster is a subset of the files grouped through logical organization, and determining if any of the files are arranged in clusters comprises referencing a security information resource file contained within a start file, wherein the security information resource file comprises a cluster information metadata expression indicating the files that compose the cluster, a signature location metadata expression indicating a location of a signature for the cluster; [[:]]

determining if ~~an~~ the application start file has a record that includes one of a reference to an expression having a location of the signature, and the expression, wherein the start file carries application run parameters and references an application boot file to start execution of the supplemental television content application ~~is a file that describes parameters to execute an associated application~~;

reading from the expression the location of a file having a signature of a cluster for each cluster, wherein the reading operation further comprises reading whether there are any delegates for any of the clusters, and determining if a signature is valid based on the delegates wherein a delegate is an entity that is authorized to sign portions of the application in addition to a main signer;

determining if the signatures can be verified;

determining the identify of all clusters that comprise the application;

~~for each cluster,~~

~~determining the location of the signature of the cluster files that compose the cluster by a signature location metadata expression;~~

~~determining the files that compose the cluster by a cluster information metadata expression;~~

determining a delegate name and constraints imposed on the authority of the delegate, wherein the constraints comprise time boundaries; and

verifying the integrity of the files in the cluster by operations including verifying the signature.

47. (Previously Canceled)

48. (Previously Presented) The computer readable media of claim 46 wherein each of the files composing a cluster is stored in one of

the expression, and

a file storing a signature.

49. (Previously Presented) The computer readable media of claim 46 wherein each signature is based on a hash of each file composing the cluster.

50. (Previously Canceled)

51. (Previously Presented) The computer readable media of claim 46 further comprising reading time version information associated with a cluster and determining if the signature may be valid based on the time version information.

52. (Previously Presented) The computer readable media of claim 46 wherein said acts further comprise determining if the files is a web page file having one of a link to a signature and a signature; reading the signature, and verifying the signature.

53. (Currently Amended) One or more computer readable media having stored thereon a plurality of instructions that, when executed by at least one processor, causes the processor to perform acts comprising:

executing a supplemental television content application comprising files, wherein the files carry code and assorted objects;

determining if supplemental television content application files compose web pages; and

if the files compose web pages, then

for each of the web pages, decoding the web page file to determine if the web page has an extensible markup language (XML) metadata comprising an <AppSecurityInfo> element indicating one of a link to a digital signature and a digital signature,

reading the signature, and

verifying the signature,

if any of the web pages lack the link to a digital signature, lack the digital signature, or the signatures is not verified then warn a user that a file has not been signed, warn the user that the signature is not valid, reject the file, or restrict access by the web page to system resources.

54. (Previously Presented) The computer readable media of claim 53, the acts further comprising:

determining if the files are arranged in a cluster;

for each cluster, determining the files that compose the cluster and the location of the signature of the cluster;

verifying the integrity of the files in the cluster by operations including verifying the signature.

55. (Currently Amended) A supplemental television content architecture comprising:

an application comprising a collection of files;

the files comprising:

a supplemental television content delivered through an interconnecting channel separate from a channel used to deliver broadcast media;

at least one of a dynamic web page coded with a signature as extensible markup language (XML) metadata or including a reverse linkage between an XML document and ~~link to~~ a signature file coded with the signature by using a link rev= tag; and

a dynamic web page coded with a security information resource file comprising a signature location metadata, and a delegate metadata,

wherein a content of the dynamic web page changes during a time interval;

wherein the signature ~~changes as~~ is calculated from a hash code of the webpage each time the web page changes,

wherein the delegate metadata comprises an identity and constraints of a delegate.

56. (New) The method of claim 12, wherein the interconnecting channel separate from the channel used to deliver broadcast media comprises an Internet connection.

57. (New) The architecture of claim 25, wherein the interconnecting channel separate from the channel used to deliver broadcast media comprises an Internet connection.

58. (New) The computer readable media of claim 42, wherein the interconnecting channel separate from the channel used to deliver broadcast media comprises n Internet connection.

59. (New) The architecture of claim 55, wherein the interconnecting channel separate from the channel used to deliver broadcast media comprises an Internet connection.